Nombre: _____ **Fecha:** _____ **Puntuación:** _____

VPN de acceso remoto

Protección de los dispositivos de los trabajadores en remoto, autenticación multifactor y configuración de túneles IPsec.

RESUMEN DE APRENDIZAJE: VPN DE ACCESO REMOTO

ALUMNO
CONDICIÓN DE ESTUDIANTE
Itinerario de defensor de redes

SEGURO
ESTADO DE LA CONEXIÓN
Proteger los paquetes de datos

ACTIVO
PROTECCIÓN CONTRA FUGAS
Protección contra fugas de DNS e IPv6

¡Hola! Este paquete de actividades te guía por las redes VPN de acceso remoto. Explorarás los túneles de cliente a sitio, los inicios de sesión multifactor, las comprobaciones del estado de los puntos finales, los límites de ancho de banda y la auditoría de seguridad mediante syslog.

PUNTOS DE CONTROL DE LA HOJA DE TRABAJO

- [ ] **Partes 1-4: Domina las configuraciones de VPN y de seguridad de redes.**
- [ ] **Partes 5-7: Resuelve crucigramas y sopas de letras.**
- [ ] **Partes 8-9: Resuelve casos prácticos y el reto de cifrado.**
- [ ] **Parte 10: Repasa las páginas de preguntas frecuentes básicas y avanzadas.**
- [ ] **Parte 11: Explora 10 datos reales interesantes.**
- [ ] **Extra: reto Piensa rápido.**

Abre la guía de las mejores VPN de VPN.com

URL: https://www.vpn.com/es/vpn/mejor-vpn-empresas/acceso-remoto/

Tu hoja de ruta de aprendizaje sobre VPN de acceso remoto

- Proteger los dispositivos de los trabajadores en remoto que acceden a los nodos de la red local.
- Configura políticas de autenticación multifactor para los inicios de sesión remotos.
- Configurar IPsec de cliente a sitio y OpenVPN.
- Audita los registros de conexión remota en busca de infracciones del control de acceso.
- Implantar comprobaciones del estado de seguridad de los dispositivos antes de conceder conexiones a la red.
- Optimizar el rendimiento del servidor para evitar el estrangulamiento del ancho de banda en el teletrabajo.

INSTRUCCIONES DE VPN DE ACCESO REMOTO

Responde a las preguntas de opción múltiple y de verdadero/falso, completa las frases con huecos usando el banco de palabras, relaciona las definiciones y resuelve el crucigrama y la sopa de letras. Aplica tus conocimientos a las comprobaciones de postura y los inicios de sesión multifactor. Termina con la actividad extra Piensa rápido.

TÚNELES CLIENTE A SITIO Y CUMPLIMIENTO DE LOS ENDPOINTS (INTRODUCCIÓN)

Las VPN de acceso remoto establecen túneles seguros de cliente a sitio para los empleados que trabajan fuera de la oficina. Proteger estas conexiones exige imponer inicios de sesión con autenticación multifactor (MFA), comprobar el cumplimiento del estado de seguridad de los equipos y auditar los registros mediante recopiladores syslog centrales.

LEE ATENTAMENTE CADA PUNTO DE CONTROL Y SELECCIONA O ESCRIBE LA RESPUESTA CORRECTA.

Punto de control 1: Reto de opción múltiple

1. ¿Qué estándar de autenticación deberían exigir los portales VPN de acceso remoto?

- A) Multifactor
- B) Un solo factor
- C) Sin cifrar
- D) Invitado local

2. ¿Qué protocolo es el estándar para proteger las conexiones de cliente a sitio del teletrabajo?

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3. ¿Qué comprobación valida que un portátil remoto esté limpio antes de conectarse?

- A) Comprobación del estado de seguridad
- B) Prueba de velocidad
- C) Prueba de ping
- D) Cantidad de memoria

4. ¿Dónde se almacenan los registros de conexión de los trabajadores remotos para las auditorías de seguridad?

- A) Servidor syslog
- B) Clave del registro
- C) Memoria del cliente
- D) Navegador web

5. ¿Qué problema surge cuando el número de trabajadores remotos supera la capacidad de ancho de banda de la pasarela?

- A) Estrangulamiento del ancho de banda
- B) Fuga de DNS
- C) Paso de negociación (handshake)
- D) Exposición de la IP

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. La autenticación multifactor añade un token de validación secundario para proteger los inicios de sesión remotos.

○ Verdadero ○ Falso

7 Pregunta 7

7. Las comprobaciones de estado permiten a los dispositivos remotos con cortafuegos desactivados acceder a servidores privados.

○ Verdadero ○ Falso

8 Pregunta 8

8. Los registros de la VPN de acceso remoto son esenciales para rastrear accesos no autorizados a la red corporativa.

○ Verdadero ○ Falso

9 Pregunta 9

9. OpenVPN e IPsec son protocolos antiguos que no cifran los datos de los clientes remotos.

○ Verdadero ○ Falso

10 Pregunta 10

10. El cuello de botella del ancho de banda de la puerta de enlace se produce cuando el tráfico remoto supera la capacidad de la tarjeta de conexión.

○ Verdadero ○ Falso

Punto de control 3: Inserción de términos clave

Lee cada una de las frases siguientes y rellena el espacio en blanco con el término correcto del banco de palabras.

1. Para proteger los portales corporativos, los inicios de sesión remotos deben exigir la autenticación _____ .

2. Los clientes remotos cifran el contenido del túnel de datos mediante protocolos estándar como _____ .

3. Los dispositivos deben superar una comprobación de _____ **seguridad antes de obtener acceso a la red.**

4. Los registros de acceso auditables se transmiten de forma continua a un servidor _____ **central.**

5. El tráfico intenso en horario laboral puede provocar congestión del _____ **en la puerta de enlace.**

6. Los controladores de adaptadores virtuales gestionan la _____ **de cliente a sede en Windows y macOS.**

BANCO DE PALABRAS DE VOCABULARIO

ANCHO DE BANDA CIFRADO CORTAFUEGOS MULTIFACTOR OPENVPN POSTURA SYSLOG TUNELIZACIÓN

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos clave

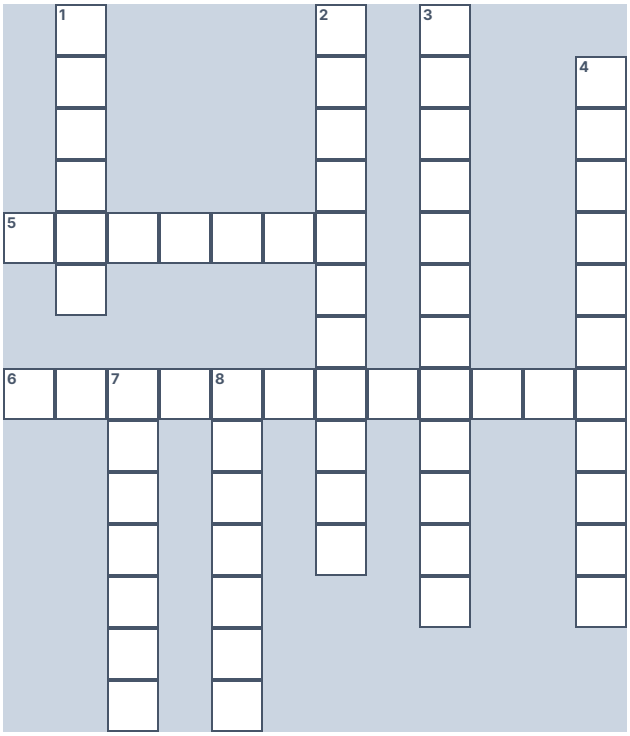
RELACIÓN DE DEFINICIONES

Relaciona cada término de vocabulario de la izquierda con su definición correcta de la derecha escribiendo la letra correspondiente (A-H) en la casilla rellenable.

☐	1. MULTIFACTOR	A	Encapsular los datos en una ruta segura.
☐	2. OPENVPN	B	Recopilador central de registros de seguridad.
☐	3. ESTADO DE SEGURIDAD	C	Límite de capacidad de datos de la red.
☐	4. SYSLOG	D	Protocolo estándar de cliente a sitio.
☐	5. ANCHO DE BANDA	E	Validación remota del estado del dispositivo.
☐	6. CIFRADO	F	Reglas del sistema de filtrado de tráfico.
☐	7. TUNELIZACIÓN	G	Codificación criptográfica de los paquetes.
☐	8. CORTAFUEGOS	H	Seguridad de inicio de sesión que requiere tokens adicionales.

Punto de control 5: Crucigrama

Resuelve el crucigrama escribiendo letras en las casillas blancas activas. Los números corresponden a las pistas de abajo.



HORIZONTALES

5. Validación del estado de seguridad del dispositivo remoto (7)

6. Límite de capacidad de datos de la red (12)

VERTICALES

1. Recolector central de registros de seguridad (6)

2. Reglas del sistema de filtrado de tráfico (11)

3. Encapsulación de los datos en una ruta segura (12)

4. Seguridad de inicio de sesión que exige tokens adicionales (11)

7. Codificación criptográfica de los paquetes (7)

8. Protocolo estándar de cliente a sede (client-to-site) (7)

Punto de control 5, alternativa: Pistas accesibles del crucigrama

Los usuarios de lectores de pantalla y de teclado pueden escribir las respuestas del crucigrama directamente en los campos de texto de abajo.

HORIZONTALES

5 horizontal: Validación del estado de seguridad del dispositivo remoto (7 letras):

6 horizontal: Límite de capacidad de datos de la red (12 letras):

VERTICALES

1 vertical: Recolector central de registros de seguridad (6 letras):

2 vertical: Reglas del sistema de filtrado de tráfico (11 letras):

3 vertical: Encapsulación de los datos en una ruta segura (12 letras):

4 vertical: Seguridad de inicio de sesión que exige tokens adicionales (11 letras):

7 vertical: Codificación criptográfica de los paquetes (7 letras):

8 vertical: Protocolo estándar de cliente a sede (client-to-site) (7 letras):

Punto de control 6: Sopa de letras

Encuentra los 8 términos clave del vocabulario ocultos en la cuadrícula de abajo. Las palabras pueden estar en horizontal, en vertical o en diagonal.

N	I	R	Z	S	F	Q	V	F	A	A	Q	O	N	P
O	T	X	Q	K	N	P	V	N	E	P	O	R	T	R
I	D	G	N	Y	B	G	R	P	O	S	T	U	R	A
C	X	O	W	C	J	A	R	Z	Y	Y	L	G	I	N
A	Q	L	K	I	M	M	T	O	H	P	Q	H	M	Z
Z	A	S	O	F	V	G	U	C	Y	R	Y	B	U	H
I	M	Y	Z	R	G	K	Ñ	P	Ñ	W	C	M	L	Z
L	Y	S	G	A	Y	O	W	U	L	U	P	B	T	Ñ
E	V	T	M	D	H	U	D	Y	U	K	R	B	I	W
N	Z	Y	M	O	R	Q	X	I	O	D	A	D	F	K
U	A	N	C	H	O	D	E	B	A	N	D	A	A	Q
T	V	W	W	L	J	I	T	I	G	B	F	I	C	L
T	R	C	O	R	T	A	F	U	E	G	O	S	T	V
Q	Z	E	I	F	R	C	A	L	P	C	Z	M	O	K
V	R	U	A	S	W	K	M	M	H	H	N	I	R	Q

LISTA DE PALABRAS DE VOCABULARIO

MULTIFACTOR OPENVPN POSTURA SYSLOG ANCHODEBANDA CIFRADO TUNELIZACION CORTAFUEGOS

Punto de control 6, alternativa: Relación de vocabulario accesible

Relaciona cada uno de los 8 términos de vocabulario de la sopa de letras con su definición correcta escribiendo la letra (A-H) en el espacio en blanco.

TÉRMINOS DE VOCABULARIO	DEFINICIONES Y CAMPOS DE RELACIÓN
A. MULTIFACTOR	_____ 1. Recolector central de registros de seguridad.
B. OPENVPN	_____ 2. Reglas del sistema de filtrado de tráfico.
C. POSTURA	_____ 3. Encapsulación de los datos en una ruta segura.
D. SYSLOG	_____ 4. Codificación criptográfica de los paquetes.
E. ANCHODEBANDA	_____ 5. Protocolo estándar de cliente a sede (client-to-site).
F. CIFRADO	_____ 6. Límite de capacidad de datos de la red.
G. TUNELIZACION	_____ 7. Validación del estado de seguridad del dispositivo remoto.
H. CORTAFUEGOS	_____ 8. Seguridad de inicio de sesión que exige tokens adicionales.

Punto de control 7: Reto de palabras desordenadas

Ordena las letras de abajo para descubrir conceptos clave de esta hoja de trabajo. Escribe tus respuestas en los campos proporcionados.

1. IAOUFCMTLRT
2. PSARUTO
3. ANBEDACDAONH
4. OALNZNIICTUE
5. VNNEOPP
6. OLSSGY
7. CDAOIRF
8. GUSFRCAOOET

Actividad extra: Piensa rápido

3 RESPUESTAS POR CATEGORÍA. GANA QUIEN COMPLETE PRIMERO LA LISTA.

1	Mitos sobre las VPN			
2	Palabras que describen Zero Trust			
3	Programas de oficina que conoces			
4	Normas para teletrabajar de forma segura			
5	Cosas que puede ver tu proveedor de internet			
6	Servicios VPN que conoces			
7	Lugares desde los que trabajan los empleados			
8	Herramientas que una empresa usa todos los días			
9	Puestos de un departamento de TI			
10	Dispositivos que podría tener un empleado			
11	Datos que una empresa debe proteger			
12	Cosas que hacer tras una brecha de seguridad			
13	Cosas que pueden interrumpir una videollamada			
14	Formas de iniciar sesión de forma segura			
15	Razones para dar una VPN a los empleados			

Punto de control 8: Casos prácticos de VPN y redes

Aplica los conceptos que has aprendido para resolver los escenarios reales que aparecen a continuación.

CASO PRÁCTICO 1: OBLIGATORIEDAD DE LA MFA



Escenario: Un analista de negocio intenta iniciar sesión en la base de datos de su empresa mientras teletrabaja. Introduce su nombre de usuario y contraseña correctos, pero el portal VPN bloquea el acceso y le pide el código de un token físico.

Pregunta de debate: ¿qué política de seguridad impone este paso de doble verificación?

CASO PRÁCTICO 2: CUMPLIMIENTO DE LA POSTURA DE SEGURIDAD



Escenario: Un contratista conecta su portátil personal a la red corporativa remota. El cliente VPN corta la conexión de inmediato y avisa al usuario de que las definiciones de su antivirus están desactualizadas.

Pregunta de debate: ¿Qué comprobación especializada de la pasarela VPN bloqueó este intento de conexión?

Punto de control 9: Descifrar el código

Un ingeniero de redes protege los canales de enrutamiento y los túneles de los clientes. Usa la clave de letras y números de abajo para descifrar el mensaje escribiendo las letras correspondientes en los espacios en blanco.

CLAVE DE CIFRADO DE LETRAS A NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9
J=10 K=11 L=12 M=13 N=14 Ñ=15 O=16 P=17 Q=18
R=19 S=20 T=21 U=22 V=23 W=24 X=25 Y=26 Z=27

23	17	14		4	5		1	3	3	5	20	16		19	5	13	16	21	16

17	19	16	21	5	7	5		5	18	22	9	17	16	20

4	9	20	17	5	19	20	16	20

Mensaje descifrado:

CONSEJO: CADA NÚMERO REPRESENTA LA POSICIÓN DE ESA LETRA EN EL ALFABETO (P. EJ., 1 = A, 2 = B, 27 = Z).

Punto de control 10: Preguntas frecuentes básicas sobre VPN (Parte A)

Repasa las preguntas y respuestas más habituales sobre las redes privadas virtuales (VPN) y la tunelización.

Q1: ¿Qué es una VPN de acceso remoto?

Un método de conexión seguro que permite a los empleados que trabajan fuera de la oficina conectarse directamente a los servidores privados de la empresa.

Q2: ¿Por qué una VPN de cliente a sitio es diferente de una de sitio a sitio?

El modelo cliente a sitio conecta dispositivos de usuarios individuales, mientras que el de sitio a sitio enlaza oficinas físicas completas.

Q3: ¿Qué es una comprobación de postura del dispositivo?

Un análisis que comprueba el estado de seguridad de un dispositivo remoto (antivirus, nivel de parches del sistema operativo) antes de concederle acceso.

Q4: ¿Por qué se utiliza OpenVPN para el acceso remoto?

Por su sólido protocolo de seguridad, su compatibilidad multiplataforma y su capacidad para gestionar conexiones individuales.

Q5: ¿Cómo protege la MFA el acceso remoto?

Añade un token de verificación secundario, lo que impide el acceso aunque las contraseñas de los empleados se filtren o se roben.

Punto de control 10: Preguntas frecuentes básicas sobre VPN (Parte B)

Repasa las preguntas y respuestas más habituales sobre las redes privadas virtuales (VPN) y la tunelización.

Q6: ¿Qué es un servidor syslog?

Un repositorio de registros centralizado que almacena los eventos de conexión, los inicios de sesión y las alertas del sistema para las auditorías de cumplimiento.

Q7: ¿Qué causa la saturación del ancho de banda?

Cuando la demanda total de ancho de banda de los empleados remotos supera el límite de velocidad de internet de la pasarela corporativa.

Q8: ¿Puedo conectar el ordenador de casa a una VPN del trabajo?

Solo si el dispositivo supera las auditorías corporativas de comprobación de estado y está autorizado por los administradores de TI.

Q9: ¿Qué es la encapsulación de red?

La encapsulación de los paquetes de datos en tránsito dentro de encabezados de protocolo cifrados para proteger la transmisión.

Q10: ¿Cómo optimiza el túnel dividido el acceso remoto?

Permite a los empleados usar su ISP local para la navegación habitual mientras los archivos de trabajo se enrutan a través de la VPN.

Punto de control 10: Preguntas frecuentes avanzadas sobre VPN (Parte C)

Explora aspectos técnicos avanzados de los protocolos de tunelización VPN, las integraciones con clientes móviles y el despliegue empresarial.

Q1: ¿Cómo mejora la autenticación basada en certificados el acceso remoto?

Vincula los permisos de conexión a certificados digitales locales preinstalados, lo que bloquea los dispositivos no gestionados o no autorizados.

Q2: ¿Qué riesgo de seguridad supone el túnel dividido en el teletrabajo?

Crea un posible puente a través del cual un dispositivo local comprometido puede introducir amenazas externas en la red privada.

Q3: ¿Cómo inspeccionan las comprobaciones de postura la configuración del registro?

El cliente VPN ejecuta scripts locales que consultan rutas del registro para verificar si el software de seguridad corporativo está en funcionamiento.

Q4: ¿Por qué syslog utiliza de forma predeterminada el puerto UDP 514?

Para transmitir los registros rápidamente y con la mínima sobrecarga, aunque las configuraciones seguras exigen ahora la encapsulación TLS sobre TCP.

Q5: ¿Cómo resuelven las empresas los cuellos de botella de ancho de banda en la pasarela?

Implementando balanceadores de carga y distribuyendo el tráfico remoto entre nodos de servidor regionales.

Punto de control 10: Preguntas frecuentes avanzadas sobre VPN (Parte D)

Explora aspectos técnicos avanzados de los protocolos de tunelización VPN, las integraciones con clientes móviles y el despliegue empresarial.

Q6: ¿Cuál es la función de los adaptadores virtuales TAP/TUN en los clientes remotos?

Actúan como tarjetas de red virtuales y enrutan el tráfico TCP/IP del dispositivo directamente al túnel VPN cifrado.

Q7: ¿Cómo favorece IKEv2 MOBIKE la movilidad de las plantillas que trabajan en remoto?

Actualiza dinámicamente las asociaciones de direcciones IP, lo que mantiene la VPN activa mientras el usuario pasa del Wi-Fi a los datos móviles.

Q8: ¿Cuál es la diferencia entre el enrutamiento de túnel dividido y el de túnel completo?

El enrutamiento completo obliga a que todo el tráfico de internet del dispositivo pase por la VPN, mientras que el enrutamiento dividido solo envía las IP de destino corporativas.

Q9: ¿Cómo gestionan los dispositivos NAT las conexiones VPN remotas?

Asignando rangos de puertos locales a direcciones IP públicas de la puerta de enlace para enrutar los paquetes de datos cifrados de vuelta.

Q10: ¿Qué normas de cumplimiento exigen auditar el acceso remoto?

Normas como HIPAA, SOC 2 y PCI DSS exigen registrar y supervisar todas las sesiones de conexión remota.

Parte 11: 10 datos reales sobre las VPN y su aplicación

Repasa datos reales sobre velocidades de cifrado de VPN, auditorías de protocolos, conectividad móvil y teletrabajo en empresas.

1. PERSPECTIVA SOBRE VPN
Las VPN de acceso remoto establecen túneles seguros de cliente a sitio para los trabajadores fuera de la oficina.

2. PERSPECTIVA SOBRE VPN
Las normas de cumplimiento exigen la autenticación multifactor para proteger los portales empresariales remotos.

3. PERSPECTIVA SOBRE VPN
Las comprobaciones de estado verifican los ajustes de seguridad locales del cliente antes de conceder acceso a la red privada.

4. PERSPECTIVA SOBRE VPN
Los servidores Syslog reúnen los registros de conexión para auditar y detectar intentos de acceso no autorizado.

5. PERSPECTIVA SOBRE VPN
Los cuellos de botella del ancho de banda de la puerta de enlace se producen cuando la demanda total de tráfico remoto supera los límites de internet del servidor.

6. PERSPECTIVA SOBRE VPN
Los adaptadores de red virtuales encapsulan las consultas de red del sistema operativo dentro de protocolos seguros.

7. PERSPECTIVA SOBRE VPN
La compatibilidad con MOBIKE permite a los clientes remotos cambiar de red sin que se corte el túnel VPN.

8. PERSPECTIVA SOBRE VPN
El enrutamiento de túnel completo protege todo el tráfico de internet del trabajador, pero aumenta la carga de la puerta de enlace corporativa.

9. PERSPECTIVA SOBRE VPN
La autenticación por certificado vincula la autorización de la conexión VPN directamente al hardware gestionado por la empresa.

10. PERSPECTIVA SOBRE VPN
Marcos como SOC 2 y PCI DSS esperan que se registren y supervisen las sesiones de acceso remoto.

Referencias técnicas y fuentes

La guía de estudio y los pasatiempos interactivos se han elaborado a partir de estándares técnicos, especificaciones y marcos normativos internacionales.

REFERENCIAS ACADÉMICAS Y DEL SECTOR

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

Clave de respuestas: Punto de control 1 – Opción múltiple

1 **Tokens de inicio de sesión** SEGURIDAD MFA **Respuesta correcta: A**

NOTA PARA DOCENTES

La autenticación multifactor impone una verificación secundaria en los inicios de sesión. Cita: MFA Implementation.

2 **Túnel OpenVPN** CLIENTE A SITIO **Respuesta correcta: A**

NOTA PARA DOCENTES

OpenVPN es un protocolo estándar para proteger túneles de cliente a sitio. Cita: OpenVPN Client.

3 **Auditorías de estado de seguridad** COMPROBACIÓN DEL DISPOSITIVO **Respuesta correcta: A**

NOTA PARA DOCENTES

Las comprobaciones de estado analizan los dispositivos para verificar que tienen cortafuegos y antivirus activos. Cita: Posture Compliance.

4 **Agregador de registros** SERVIDOR SYSLOG **Respuesta correcta: A**

NOTA PARA DOCENTES

Los servidores Syslog recopilan registros de eventos de seguridad para supervisar las infracciones de acceso. Fuente: Syslog Standard.

5 **Desbordamiento de la tarjeta** CUELLO DE BOTELLA EN LA PUERTA DE ENLACE **Respuesta correcta: A**

NOTA PARA DOCENTES

El cuello de botella del ancho de banda de la puerta de enlace se produce cuando el tráfico de los usuarios supera los límites del servidor. Cita: Capacity Planning.

Clave de respuestas: Punto de control 2 – Verdadero o falso

6 **Tokens de inicio de sesión** COMPROBACIONES MFA — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

La autenticación multifactor impone una verificación secundaria en los inicios de sesión. Cita: MFA Implementation.

7 **Pregunta 7** — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Las comprobaciones de postura bloquean los dispositivos con el cortafuegos o el antivirus desactivados, por lo que se les deniega el acceso.

8 **Agregador de registros** SERVIDOR SYSLOG — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los servidores Syslog recopilan registros de eventos de seguridad para supervisar las infracciones de acceso. Fuente: Syslog Standard.

9 **Pregunta 9** — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

OpenVPN e IPsec son protocolos actuales que sí cifran el tráfico de los clientes remotos.

10 **Desbordamiento de la tarjeta** CUELLO DE BOTELLA EN LA PUERTA DE ENLACE — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

El cuello de botella del ancho de banda de la puerta de enlace se produce cuando el tráfico de los usuarios supera los límites del servidor. Cita: Capacity Planning.

Claves de vocabulario y rúbrica de calificación

Rúbrica de calificación para docentes: concede 1 punto por cada relación correcta (8 puntos en total) y por cada término de contexto (6 puntos en total).

PUNTO DE CONTROL 4: SOLUCIÓN DE LA RELACIÓN DE CONCEPTOS

H 1. MULTIFACTOR	D 2. OPENVPN	E 3. ESTADO DE SEGURIDAD	B 4. SYSLOG
C 5. ANCHO DE BANDA	G 6. CIFRADO	A 7. TUNELIZACIÓN	F 8. CORTAFUEGOS

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 MULTIFACTOR	2 OPENVPN	3 POSTURA	4 SYSLOG
5 ANCHO DE BANDA	6 TUNELIZACIÓN		

PUNTO DE CONTROL 6, ALTERNATIVA: SOLUCIÓN DE LA RELACIÓN DE PALABRAS

1 D – SYSLOG	2 H – CORTAFUEGOS	3 G – TUNELIZACION	4 F – CIFRADO
5 B – OPENVPN	6 E – ANCHODEBANDA	7 C – POSTURA	8 A – MULTIFACTOR

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar MULTIFACTOR, OPENVPN y ESTADO DE SEGURIDAD con sus propias palabras y dar un ejemplo de cada uno.

Casos prácticos:
Pide a los estudiantes que justifiquen sus recomendaciones con datos de la hoja de trabajo y no con suposiciones.

Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

N	I	R	Z	S	F	Q	V	F	A	A	Q	O	N	P
O	T	X	Q	K	N	P	V	N	E	P	O	R	T	R
I	D	G	N	Y	B	G	R	P	O	S	T	U	R	A
C	X	O	W	C	J	A	R	Z	Y	Y	L	G	I	N
A	Q	L	K	I	M	M	T	O	H	P	Q	H	M	Z
Z	A	S	O	F	V	G	U	C	Y	R	Y	B	U	H
I	M	Y	Z	R	G	K	Ñ	P	Ñ	W	C	M	L	Z
L	Y	S	G	A	Y	O	W	U	L	U	P	B	T	Ñ
E	V	T	M	D	H	U	D	Y	U	K	R	B	I	W
N	Z	Y	M	O	R	Q	X	I	O	D	A	D	F	K
U	A	N	C	H	O	D	E	B	A	N	D	A	A	Q
T	V	W	W	L	J	I	T	I	G	B	F	I	C	L
T	R	C	O	R	T	A	F	U	E	G	O	S	T	V
Q	Z	E	I	F	R	C	A	L	P	C	Z	M	O	K
V	R	U	A	S	W	K	M	M	H	H	N	I	R	Q

SOLUCIÓN DEL CRUCIGRAMA

	S					C		T						
	Y					O		U					M	
	S					R		N					U	
	L					T		E					L	
P	O	S	T	U	R	A		L					T	
	G					F		I					I	
						U		Z					F	
A	N	C	H	O	D	E	B	A	N	D	A		A	
		I		P		G		C					C	
		F		E		O		I					T	
		R		N		S		O					O	
		A		V				N					R	
		D		P										
		O		N										

GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

5 horizontal: POSTURA Validación del estado de seguridad del dispositivo remoto (7 letras)

6 horizontal: ANCHODEBANDA Límite de capacidad de datos de la red (12 letras)

VERTICALES

1 vertical: SYSLOG Recolector central de registros de seguridad (6 letras)

2 vertical: CORTAFUEGOS Reglas del sistema de filtrado de tráfico (11 letras)

3 vertical: TUNELIZACION Encapsulación de los datos en una ruta segura (12 letras)

4 vertical: MULTIFACTOR Seguridad de inicio de sesión que exige tokens adicionales (11 letras)

7 vertical: CIFRADO Codificación criptográfica de los paquetes (7 letras)

8 vertical: OPENVPN Protocolo estándar de cliente a sede (client-to-site) (7 letras)

Clave de soluciones de palabras desordenadas y del cifrado

Clave de calificación de la actividad de ordenar letras del vocabulario y del Reto del código secreto.

CLAVE DE LAS PALABRAS DESORDENADAS

1. I A O U F C M T L R T — **MULTIFACTOR**
2. P S A R U T O — **POSTURA**
3. A N B E D A C D A O N H — **ANCHODEBANDA**
4. O A L N Z N I I C T U E — **TUNELIZACION**
5. V N N E O P P — **OPENVPN**
6. O L S S G Y — **SYSLOG**
7. C D A O I R F — **CIFRADO**
8. G U S F R C A O O E T — **CORTAFUEGOS**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"VPN DE ACCESO REMOTO PROTEGE EQUIPOS DISPERSOS"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Obligatoriedad de la MFA

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un analista de negocio intenta iniciar sesión en la base de datos corporativa mientras teletrabaja. Introduce su usuario y contraseña correctos, pero el portal VPN bloquea el acceso y le pide un código de un token físico.
- Estrategia y solución recomendadas: el portal VPN corporativo impone una política estricta de autenticación multifactor (MFA) para proteger los inicios de sesión remotos.

B Caso práctico 2: Cumplimiento de la postura de seguridad

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un contratista conecta su portátil personal a la red corporativa remota. El cliente VPN corta la conexión de inmediato y le avisa de que sus definiciones de antivirus están desactualizadas.
- Estrategia y solución recomendadas: la pasarela de acceso remoto realizó una comprobación del estado de seguridad del equipo y bloqueó el dispositivo por tener configuraciones de seguridad desactualizadas.